Remarks/Arguments

Extension of Time

A petition for a two month extension of the period within which to respond to the Office Action mailed May 20, 2004 is enclosed. The extended period for response expires on October 20, 2004.

Amendments to the Specification

Minor revisions to the specification are made. With respect to the revisions made to the equations on pages 24, 27 and 28, in view of the difficulty of showing the revisions, applicant has attached three annotated pages showing the revisions in red ink.

Claim Status

Claims 1-20 were presented in this application. Claims 4, 8 and 10 are amended and claims 21-23 are added. Accordingly, after entry of this amendment, claims 1-23 are pending.

Art-Based Rejections

In paragraphs 1-12 of the Office Action, claims 1, 2, 4, and 12-20 were rejected under 35 U.S.C. § 102(b) as being anticipated by Tanaka, "Security Certified Identity-based Non-Interactive Key Sharing."

In paragraphs 13-21 of the Office Action, claims 3, 5, 6, and 8-11 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Tanaka in view if Miyaji et al., USPN 5,272,755.

The Applicant respectfully traverses the rejections, however, in order to expedite prosecution, the Applicant has amended the claims, and respectfully submits that the claims are patentable in light of the arguments presented herein.

The Tanaka Reference

The Tanaka reference discloses security certified identity-based non-interactive key sharing. The security depends on the difficulty of factoring. See Abstract.

The Miyaji Reference

The Miyaji reference discloses a public key cryptosystem with an elliptic curve. The step of informing public data includes the stages of choosing d as a positive integer such that gives an imaginary quadratic field a small class number, choosing p as a prime number so that an elliptic curve will have a j-invariant as a solution modulo p for a class polynomial which is fixed by d. See Abstract.

The Claims are Patentable over the Cited Reference

The claims of the present invention describe a cryptographic communication method for communicating information through a ciphertext between entities. A method in accordance with the present invention comprises generating a secret key of each entity by using mapping at a point on an algebraic curve based on identity information of each entity and secret information, generating at a first entity a first common key by using the secret key of the first entity and a public key obtained by mapping at a point on the algebraic curve based on identity information of a second entity, encrypting at the first entity a plaintext into a ciphertext by using the generated first common key and transmitting the ciphertext to the second entity, generating at the second entity the same second common key as the first common key by using the secret key of the second entity and a public key obtained by mapping at a point on the algebraic curve based on identity information of the first entity, and decrypting at the second entity the transmitted ciphertext into a plaintext by using the generated second common key.

The cited references do not teach nor suggest the limitations of the claims of the present invention. Specifically, the cited references do not teach nor suggest at least the limitation of generating a secret key of each entity by using mapping at a point on an algebraic curve as recited in the claims of the present invention.

The Tanaka reference discloses a method of key sharing without preliminary communication by using identification information of each entity. However, the method of sharing the key (method for obtaining a secret key, a public key and a common key) is completely different. Tanaka teaches substituting identification information of an entity into a one-way function f to obtain two types of hash values

and generating a secret key by using the hash values and random numbers. See equations 1-4 in column 1. Tanaka performs mapping on a finite field based on the identification information, where the equations are used for conversion into a scalar (integer) amount. No mapping onto an algebraic curve is performed. As such, Tanaka does not teach nor suggest at least the limitation of generating a secret key of each entity by using mapping at a point on an algebraic curve as recited in the claims of the present invention.

The ancillary Miyaji reference does not remedy the deficiencies of the primary Tanaka reference. Specifically, Miyaji teaches using a property of converting a discrete logarithm onto an elliptic curve into a discrete logarithm on a finite field. Moreover, Miyaji's intended purpose and usage of pairing is completely different from that of the present invention. Miyaji uses pairing only for analyzing cryptography (security evaluation), unlike the present invention, which uses pairing for a key sharing method. As such, neither reference, alone or in any combination, teaches or suggests at least the limitation of generating a secret key of each entity by using mapping at a point on an algebraic curve as recited in the claims of the present invention.

Thus, it is submitted that independent claims 1, 2, 4, 8, 10, and 12-20 are patentable over the cited references. Claims 3, 5-7, 9, 11, and 21-23 are also patentable over the cited reference, not only because they contain all of the limitations of the independent claims, but because claims 3, 5-7, 9, 11, and 21-23 also describe additional novel elements and features that are not described in the prior art.

Conclusion

This application is now believed to be in form for allowance. The examiner is invited to telephone the undersigned to resolve any issues that remain after entry of this amendment. Any fees due with this response may be charged to our Deposit Account No. 50-1314.

Respectfully submitted,
HOGAN & HARTSON L.L.P.

Date: October 15, 2004

By: _____
Troy M. Schmelzer
Registration No. 36,667
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Phone: 213-337-6700
Fax: 213-337-6701

[Safety related to Common Key between Entities]

An attack in which n entities colluding each other counterfeit the common key between the entities A and C will be considered. If it is assumed that the public key P_c of the entity C can be expressed by linear combination of the public keys of other entities as in the above equation (15), common keys K_{ac} and K_{ca} between both entities A and C are exposed as in the following equations (25) and (26), and so is the case in which the secret key S_c of the entity C can be expressed by the linear combination.

$$\begin{aligned} K_{ac} &= \langle\!\langle S_a, P_c \rangle\!\rangle \\ &= \langle\!\langle S_a, u_1 P_1 + u_2 P_2 + \cdots + u_n P_n \rangle\!\rangle \\ &= \langle\!\langle S_a, P_1 \rangle\!\rangle^{u_1} \langle\!\langle S_a, P_2 \rangle\!\rangle^{u_2} \cdots \langle\!\langle S_a, P_n \rangle\!\rangle^{u_n} \\ &= K_{a1}^{u_1} K_{a2}^{u_2} \cdots K_{an}^{u_n} \cdots (25) \end{aligned}$$

$$K_{ca} = K_{1a}^{-u_1} K_{2a}^{-u_2} \cdots K_{na}^{-u_n} \cdots (26)$$

However, it is necessary to solve the extended elliptic discrete logarithm problem to obtain the coefficient u_i in the above equation (15). Accordingly, such an attack is hard to perform.

The entity A cannot counterfeit a common key K_{bc} between other entities from the self-public key P_a and self-secret key S_a if any. The reason is that the secret keys S_b and S_c are secret information about the entities B and C which cannot be obtained if there is no secret information r. Accordingly, any entity cannot counterfeit the common key K_{bc}.

$$
\begin{aligned}
K_{ab} &= \overrightarrow{S_a}\,\overrightarrow{P_b}^{t} \\
&= \overrightarrow{P_a}\,R\,\overrightarrow{P_b}^{t} \\
&= \left(P_{a1}\,P_{a2}\cdots P_{an}\right)\begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nn} \end{pmatrix}\begin{pmatrix} P_{b1} \\ P_{b2} \\ \vdots \\ P_{bn} \end{pmatrix} \\
&= \left(\sum_{i=1}^{n} r_{i1}P_{ai} \sum_{i=1}^{n} r_{i2}P_{ai} \cdots \sum_{i=1}^{n} r_{in}P_{ai}\right)\begin{pmatrix} P_{b1} \\ P_{b2} \\ \vdots \\ P_{bn} \end{pmatrix} \\
&= \prod_{j=1}^{n}\left\langle\!\left\langle \sum_{i=1}^{n} r_{ij}P_{ai}, P_{bj} \right\rangle\!\right\rangle \\
&= \prod_{j=1}^{n}\prod_{i=1}^{n}\left\langle\!\left\langle P_{ai}, P_{bj} \right\rangle\!\right\rangle^{r_{ij}} \qquad \cdots (30)
\end{aligned}
$$

Moreover, the entity B generates a common key K_{ba} to the entity A in the same manner. In the case in which the comparative relationship in size between the ID information of the entities A and B is taken into consideration as in the first example according to the above-mentioned embodiment, $K_{ab} = K_{ba}$ is set so that the same common key can be shared.

Next, safety according to the present embodiment will be taken into consideration.

[Safety related to Secret Information of Center]

A secret matrix R of the center is obtained from the public key vector P_c and the secret key vector S_c of an entity C equivalently to the solution of the extended elliptic discrete logarithm problem with difficulty.

$<P_{ai}, P_{bj}>$ $(1 \leq i, j \leq n)$ is calculated from the public key vector P_a of the entity A and the public key vector P_b of the entity B and each component r_{ij} $(1 \leq i, j \leq n)$ of the matrix R is obtained from the calculated $<P_{ai}, P_{bj}>$ and the common key K_{ab} shown in the following equation (31) equivalently to the extended discrete logarithm problem and the discrete logarithm problem in the same manner as the equivalence of the extended elliptic discrete logarithm problem to the elliptic discrete logarithm problem.

$$K_{ab} = \prod_{j=1}^{n} \prod_{i=1}^{n} \langle\langle P_{ai}, P_{bj} \rangle\rangle^{r_{ij}} \quad \cdots (31)$$

As described above, the secret information (symmetrical matrix R) of the center 1 is not exposed.

[Safety related to Secret Key of Entity]

An attack in which n entities colluding each other counterfeit the secret key vector S_c of the entity C will be considered. If it is assumed that the public key vector P_c of the entity C can be expressed by linear combination of the public key vectors of other entities as in the following equation (32), the following equation (33) is established if the linear combination is substituted for the above equation (29). Therefore, the